Pour une troisième génération de législation de protection des données

Poullet, Yves

Published in:
Jusletter

Publication date:
2005

Document Version
le PDF de l'éditeur

Yves Poullet

Pour une troisième génération de réglementations de protection des données

Le donné technologique s´est profondément modifié avec l´apparition de réseaux numériques aux capacités de plus en plus importantes, tous interconnectés et dont l´utilisation, de plus en plus conviviale fondée sur des protocoles de communication universels, s´appuie en outre sur des terminaux dont la nature se diversifie et dont certains se caractérisent par des performances en croissance exponentielle.

Table des matières

[Rz 1] Cette (r)évolution technologique est loin d´être close. Ainsi, les technologies «d´intelligence ambiante» ne sont déjà plus un mythe et la nanotechnologie miniaturise les terminaux et en décuple les capacités de fonctionnement. Il s´agit et c´est le premier temps de la réflexion, d´esquisser les caractéristiques de cette évolution et les risques d´atteinte à la protection des données.

[Rz 2] Le deuxième temps de notre réflexion cherche à montrer l´insuffisance de l´approche traditionnelle des réglementations de protection des données à juguler les risques nouveaux. Ces réglementations, si les approches traditionnelles restent fondées et pleinement nécessaires, doivent – et la directive 2002/58/CE relative à la protection des données dans le secteur des communications électroniques ouvre la voie – prendre en compte comme tel le fait technologique des réseaux de la société de l´information. Ainsi est justifiée ce que nous considérons, après la première génération exprimée par l´article 8 de la Convention européenne des droits de l´ Homme et fondée sur la vie privée et la deuxième plus moderne que traduisent tant la Convention n° 108 du conseil de l´ Europe que la directive européenne 1995/46/CE de protection des données à caractère personnel, qu´une nouvelle approche est nécessaire.

[Rz 3] La troisième partie de notre réflexion aborde alors quelques principes qui permettent la pleine maîtrise de ce donné technologique nouveau et devraient inspirer cette nouvelle génération de réglementations que nous appelons de nos vœux.

I. Acte premier: Où il est affirmé la profonde vulnérabilité de l´individu du fait de l´évolution du donné technologique?

[Rz 4] Le donné technologique se caractérise par ce qu´il est convenu d´appeler la «globalisation». Sans doute, ce mot évoque-t-il aujourd´hui d´abord l´absence de frontières. Le monde est, grâce aux réseaux, devenu sans

frontières. Mon *curriculum vitae* porté sur Internet est accessible depuis les quatre coins de la planète. Les traces conscientes voire inconscientes que génère l´utilisation de mon ordinateur, circulent *via* les réseaux et peuvent être collectées, traitées en de multiples endroits lointains, connus ou inconnus de la personne concernée.

[Rz 5] Mais la globalisation peut avoir un autre sens.

[Rz 6] L´ utilisation des réseaux jusqu´il y a peu réservée à des usages professionnels et à partir d´un point fixe rythme désormais notre vie quotidienne. Se multiplient les usages humains ayant recours à ces réseaux (lire un journal, commander un bien ou un service, regarder la TV, louer une vidéo cassette, chercher de l´information, placer ou lire une petite annonce, consulter son compte en banque, effectuer un paiement non liquide, …) et les réseaux mobiles permettront demain à notre frigo de commander la boisson qui vient à manquer, au propriétaire de surveiller de son lieu de vacances ce qui se passe chez lui, à la maman de vérifier en ligne la température du bébé laissé à la crèche et de vérifier le respect par le personnel de la crèche des horaires des repas…Les applications RFID [1] sont plus impressionnantes encore comme en témoignent les premières expériences d´intelligence ambiante´ [2] menées par certaines grandes surfaces ou les discothèques [3].

[Rz 7] Les développements issus des recherches en nanotechnologies [4] devraient conduire à aller plus loin encore. Ainsi, le corps lui-même pourrait être doté de molécules qui, dotées de propriétés électriques ou chimiques particulières, pourraient fonctionner comme un terminal susceptible d´agir au sein du corps et de transmettre des informations sur le fonctionnement de nos organes [5]. L´Homme ainsi est saisi par les TIC non seulement dans son action ou ses attributs externes mais au plus profond de lui.

[Rz 8] Cette globalisation, entendue cette fois comme le développement d´outils de surveillance de toutes les activités de l´individu est permise par l´évolution à la fois des supports, des terminaux et des réseaux. Quelques réflexions à ce triple propos nous permettent de souligner les risques nouveaux encourus par la personne en matière de protection des données.

[Rz 9] La première évolution concerne les **supports d´information**. Il est coutumier à leur propos de rappeler la loi de MOORE qui établit que la performance des supports d´information double tous les dix-huit mois (soit par mille tous les quinze ans) alors que, dans le même temps le prix diminue de moitié pour une performance égale. Dans une étude pour le Conseil de l´Europe [6], nous concluions: *«il est devenu et il deviendra de plus en plus possible et de moins en moins cher d´enregistrer la vie de tous les individus de la planète (la nôtre et celle des autres …)».*

[Rz 10] A titre d´illustration, nous pouvons examiner la faisabilité de l´enregistrement de toutes les communications téléphoniques sortant d´Europe vers le monde entier. Ce n´est pas rien puisqu´il s´agit de stocker l´équivalent de cinquante milliard de minutes de télécommunications vocales [7] sur une base annuelle [8]. Si l´on considère qu´il faut environ dix mille bits par seconde pour digitaliser la voix et que l´on peut comprimer les données d´un facteur deux (ce qui est classique), on observe qu´il faudra en moyenne de l´ordre de cinq tera octets pour stocker 24 heures de trafic, ce qui à l´heure actuelle est tout à fait envisageable avec des systèmes de *disk array* où chaque disque peut stocker de l´ordre de 400 gigabytes [9]. En outre, le débit moyen de ce flux continu de centaines de milliers de communications simultanées représente un débit d´environ 0,5 gigabits par seconde, ce qui est largement supportable par une seule fibre optique de l´épaisseur d´un cheveu [10]. En d´autres termes, il serait techniquement possible de faire passer TOUT ce trafic téléphonique à travers un mince tube en verre de quelques microns d´épaisseur.

[Rz 11] Dans le commerce, on trouve actuellement des systèmes de type walkman capables d´enregistrer le contenu de l´équivalent de plusieurs centaines de CD-ROM classiques au format MP3. Les appareils photos digitaux permettent de stocker des centaines voire des milliers de photos alors que la capacité du film classique plafonne à 36 vues.

[Rz 12] Le Registre National de la Belgique qui contient la démographie de tous les belges de la naissance à leur mort ainsi que leurs professions, mariages, métiers et adresses successives [11], sans compter des données relatives aux étrangers résidents en Belgique, tiendrait aujourd´hui sans problème sur une cassette DAT de la taille d´une grosse boite d´allumettes ou sur quelques DVD. Il pourrait intégralement être transmis par fibre optique en quelques dizaines de secondes.

[Rz 13] Si cette révolution multiplie les risques d´atteinte à la protection des données, nous soulignons que le principal risque consiste du fait de la miniaturisation des supports et la difficulté de contrôler effectivement l´existence de tels traitements.

[Rz 14] Une deuxième évolution notable affecte les **équipements terminaux**. L´évolution est multiple. Elle est bien évidemment technique. Elle est d´ordre fonctionnel, ensuite. Elle concerne leur réglementation enfin.

[Rz 15] La notion de «terminal» est définie par la directive européenne sur les équipements terminaux[12] de la façon suivante: «*un produit permettant la communication, ou un composant pertinent d´un produit, destiné à être connecté directement ou indirectement par un quelconque moyen à des interfaces de réseaux publics de télécommunications (à savoir des réseaux de télécommunications servant entièrement ou en partie à la fourniture de services de télécommunications accessibles au public)*».

[Rz 16] Cette définition très large permet d´englober non seulement les ordinateurs personnels, les terminaux classiques comme le téléphone (mobile ou non), le fax ou autres mais également les RFID (Radio Frequency Identifiers)[13], les cartes à puces[14] et demain, les molécules «intelligentes» implantées au sein même du corps des individus. Ce qui caractérise les RFID dont le marché se développe à une allure exponentielle [15] est tant leur miniaturisation, que le fait qu´ils s´attachent et identifient la possession d´un objet même si indirectement elle révèle le comportement de son possesseur, soulevant la question de savoir si nos législations relatives à la protection des données «identifiant» des personnes sont applicables[16].

[Rz 17] Au-delà de ce premier phénomène, on souligne deux autres points majeurs relatifs à l´évolution des terminaux.

[Rz 18] Ainsi, premier point, la nature de l´équipement terminal est passé de l´électromécanique à une électronique programmable. En d´autres termes, le fonctionnement de l´équipement terminal est dicté par un déterminisme qui est celui non de l´utilisateur[17] mais du concepteur de l´appareil voire de tiers qui peuvent insérer dans le terminal des applicatifs permettant une utilisation à distance de ce terminal (ainsi les spyware ou l´ensemble des logiciels de mise à jour de programmes installés sur l´ordinateur)[18]. Bref, l´utilisateur d´un terminal n´a qu´une maîtrise partielle de l´ordinateur, sans que l´utilisateur ne soit à l´initiative de ces flux.

[Rz 19] Cette absence de maîtrise par l´utilisateur se double par une perte totale par l´Etat de tout contrôle des normes de production des équipements terminaux. Là où le fonctionnement du terminal «téléphone classique» était sévèrement réglementée, ce n´est plus le cas en ce qui concerne les normes techniques et fonctionnelles qui président au développement de la micro-informatique[19].

[Rz 20] Une seconde caractéristique est la «multifonctionnalité» présente dans la plupart des équipements terminaux (micro-ordinateurs mais également les nouvelles générations de GSM). La traditionnelle répartition des médias en fonction de leur capacité fonctionnelle (téléphone = transport de la voix, télévision = transport de l´image et du son, …) disparaît grâce à la numérisation de tout contenu[20] au profit d´une convergence qui permet à un terminal de fonctionner pour de multiples usages et dès lors, autorise certains acteurs comme les fournisseurs d´accès ou toute personne intervenant dans le routage voire dans l´aide à la sélection des sites de croiser désormais des données nées de l´utilisation de ces diverses fonctionnalités (ainsi, le téléphone, l´écoute de programmes radio, l´envoi de correspondance, le suivi de programmes de télévision, …).

[Rz 21] Cette polyvalence des terminaux s´explique par la polyvalence des **réseaux de communication**, capables de véhiculer des débits de plus en plus importants, ce qui permet de transmettre en temps réel des contenus de plus en plus riches comme le multimédia[21]. Une autre caractéristique de l´évolution des réseaux est sans doute le progrès rapide de la transmission sans fil qui permet la mobilité des terminaux et la continuité de leur connexion. Enfin, on souligne que la normalisation des protocoles de connexion des terminaux aux réseaux de communications électroniques échappe aux gouvernements[22].

[Rz 22] Le fait que la communication sur les réseaux modernes de communication s´opère non plus par commutation de circuits mais par paquets a des conséquences non négligeables en matière de protection des données. En d´autres termes, l´information, préalablement numérisée, est envoyée sous forme de nombreux paquets de petite taille

(typiquement de quelques dizaines de bits à quelques centaines). En fait, la commutation par paquet permet en général une utilisation optimale de la bande passante et donc de la capacité du support de télécommunication. Cette manière de faire permet un partage extrêmement souple d´un seul support de communication entre des centaines voire des milliers d´utilisateurs simultanés.

[Rz 23] Chaque paquet comporte l´adresse de l´expéditeur et l´adresse du destinataire. Sur le réseau, chaque nœud (aiguillage) qui reçoit un paquet sait sur quelle voie envoyer ce paquet sur base de son adresse de destination (on appelle cela le routage). Si, pour une raison ou pour une autre, il ne sait pas envoyer ce paquet, il peut le renvoyer au nœud qui lui a envoyé ce paquet avec une explication.

[Rz 24] Une conséquence importante est, en ce qui nous concerne, que le destinataire ou les intermédiaires intervenant dans le transport connaissent ou peuvent connaître le point d´expédition voire l´adresse de l´expéditeur, puisque celle-ci figure sur le paquet qu´il reçoit, et pour les intermédiaires le point d´émission et l´adresse de l´émetteur voire sa localisation. Ce sont les données dites de trafic ou de localisation.

1. Conclusions de l´acte 1

[Rz 25] Les conclusions de ce bref survol de l´évolution technologique s´énoncent comme suit: la protection des données ne peut être effective dans les réseaux modernes de communication que dans la mesure où les législations prennent en compte.

- **de nouveaux types de données**: A ce propos, on évoque l´existence de données liées à la possession d´objets qui, sans révéler l´identité du possesseur permettent cependant de suivre ceux-ci et de les contacter. On mentionne ensuite les données générées du simple fait de la communication qui révèlent le type, la durée, la fréquence d´utilisation des réseaux et surtout les destinataires des communications. Peut-on à leur propos parler de données à caractère personnel, au sens de l´article 2 a) de la directive 1995/46/CE? La notion d´ identité est au cœur de la définition de ce type de données. Sans doute, cette définition est-elle large dans la mesure où comme le rappelle le groupe de l´article 29, à propos des cookies ou des RFID [23], en invoquant le considérant 26, l´ «identifiabilité» se conçoit en fonction de «*l´ensemble des moyens susceptibles d´ être raisonnablement mis en place, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne»*. Outre que comme le reconnaît le groupe lui-même, cette approche même large de la notion de données à caractère personnel ne permet pas de couvrir tous les cas, elle reste théorique dans la mesure où ceux qui exploitent les données nées des cookies ou des RFID ne cherchent pas à identifier la personne concernée mais simplement à profiler[24] le détenteur d´un terminal pour décider vis-à -vis de lui de certaines actions.

- **des objets nouveaux**: on pense en particulier aux terminaux dont le fonctionnement échappe à la maîtrise de leur possesseur et dont certains peuvent être «privaticides» . A propos de ces terminaux, on note la multiplication ces dernières années des interventions du groupe de l´article 29. Nous reviendrons sur le contenu de celles-ci dans la troisième partie.

- **des acteurs nouveaux**: à savoir particulièrement ceux qui interviennent dans la connexion au réseau ou dans la transmission des communications.

[Rz 26] Le propos de l´acte II est de montrer à partir de la directive européenne 2002/58/CE la prise en compte de ces besoins nouveaux de protection et ce, au-delà de l´approche traditionnelle que consacrait la directive générale 95/46/CE.

II. Acte II: Où il est question d´une troisième génération de réglementations de protection des données

1. Trois générations de législations de protection des données: de l´article 8 la Convention européenne de 1950 à la directive 2002/58/CE.

[Rz 27] L´histoire de la protection des données prend naissance avec l´article 8 de la Convention européenne des

droits de l´homme. La disposition laisse concevoir la vie privée comme le «droit d´être laissé seul»[25], lié au droit à l´intimité des personnes. Celui de ne pas voir révéler des informations liées à sa «sphère privée», qu´elle soit physique: le domicile familial ou qu´elle soit l´expression d´une relation à autrui, le secret de la correspondance [26].

[Rz 28] La vie privée apparaît ainsi comme un concept indéfini qui ne peut se définir que de manière négative et souple. Il s´agit d´informations certes mais au-delà, d´abord de lieux (le domicile) et de relations d´un type particulier (l´espace familial et la correspondance) dont la révélation à des tiers, de la mise sur la scène publique priverait l´individu de l´espace suffisant pour pouvoir exprimer et forger sa propre personnalité et exercer ses libertés fondamentales. En d´autres termes, cette première génération de réglementation consacre la vie privée non comme une liberté en soi mais comme le minimum nécessaire à la protection de la dignité humaine et à l´exercice de libertés essentielles. Ce minimum varie et s´approfondit dans le temps. La vie privée est éminemment liée à des considérations culturelles et liée de ce fait à des valeurs changeantes et contingentes[27]. Ainsi, on peut lire sous la plume du tribunal constitutionnel espagnol[28]: «*Une exposition prolongée à des niveaux déterminés de bruits qui, objectivement, sont inévitables et insupportables, mérite de tomber sous le coup de la protection du droit à l´intimité personnelle et familiale, dans le cadre du domicile, dans la mesure où ils empêchent ou rendent particulièrement difficile le libre développement de la personnalité* …». La vie privée s´élargit ainsi au «droit à l´épanouissement» dans un environnement sain . Ce droit à l´épanouissement[29] interdit par ailleurs de limiter la vie privée *«à un ´cercle intime´ où chacun peut mener sa vie personnelle à sa guise et d´en écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l´individu de nouer et développer des relations avec ses semblables»* [30].

[Rz 29] Ce «droit» auquel il est fait référence ne fonctionne pas comme un droit subjectif mais plutôt comme une prérogative indéterminée que la personne peut faire valoir vis-à-vis de l´Etat et qui amène le tribunal saisi à vérifier au vu des circonstances si l´intérêt avancé par la personne plaignante relève bien de cette «sphère» indispensable à l´épanouissement de l´Homme, en d´autres termes de ses libertés essentielles[31] et, le cas échéant, à vérifier les conditions d´applicabilité de l´article 8.2 qui permet à l´ Etat de faire prévaloir d´autres intérêts. «*La «privacy» serait ici simplement ce que l´individu fait de la liberté qui lui est reconnue. Elle n´est pas définissable a priori: sa portée n´apparaît qu´ à travers les conflits que suscite son exercice, c´est à dire qu´elle n´est appréhendée par le droit que dans un cadre contextualisé*»[32].

[Rz 30] Dans ce débat, il est piquant de constater que la technologie a été le point de départ de cette réflexion [33] même si la disposition de 1950 s´explique par d´autres raisons historiques[34]. On ajoute - et l´exemple de la protection contre les industries polluantes en est un signe marquant – que la technologie a bien souvent été le moteur de l´évolution de la notion et de son extension. Cette réflexion nous conduit à envisager la seconde génération de législation à la fois dans ses liens avec la première génération mais également dans sa rupture avec celle-ci.

[Rz 31] La directive européenne de 1995, mais la convention n° 108 du Conseil de l´Europe l´avait précédée dès 1981, entend la protection de la vie privée de manière progressivement différente et plus précise quant aux technologies visées. Plus précise, puisque c´est à propos des seules technologies de l´information et de la communication que ces textes s´expriment. Sans doute, l´évolution de ces technologies crée-t-elle un risque d´atteinte à l´intimité sans commune mesure avec celui des méthodes de surveillance envisagées dans les années 1950 et sans doute, les premières législations de protection des données étaient-elles focalisées sur les risques d´atteinte à l´intimité des personnes et sur les dangers d´une surveillance des individus [35]. La référence exclusive à la vie privée et l´ importance des données sensibles dans les premières législations traduisent la filiation avec l´article 8 de la Convention européenne.

[Rz 32] Progressivement, il est cependant constaté que les technologies de l´information et de la communication accentuent le déséquilibre d´informations entre les personnes concernées et les responsables des traitements. Ces technologies menacent dès lors non seulement l´ intimité mais l´ensemble de libertés, ainsi, la liberté d´obtenir un crédit, un logement, celle de se déplacer, etc., en même temps qu´elles engendrent un risque important de discrimination en cas d´utilisation de données inexactes ou surtout disproportionnées. Il s´agit donc et c´est le mérite de la Convention n° 108 d´élargir le débat dans deux directions: le premier est d´instituer en vue de la protection des données à caractère personnel certaines restrictions à l´utilisation de celles-ci, de créer des obligations de sécurité et administratives à charge de ceux qui traitent des données à caractère personnel et de restreindre, d´une part, la liberté des responsables de traitements, entreprises ou associations, en particulier leur liberté d´entreprendre ou

d´associations et, d´autre part, les prérogatives d´intérêt général de l´Etat.

[Rz 33] En outre, ces lois confèrent aux personnes concernées de véritables droits subjectifs, selon la définition d´un tel droit c´est-à-dire, selon la thèse récente de Mr LEONARD, «*un pouvoir juridique spécifique reconnu par le droit objectif à son titulaire sur la chose ou la prestation qui en forme l´objet en vue de la satisfaction de ses intérêts et pour lequel il reçoit du droit objectif, le pouvoir d´imposer son respect aux tiers au moyen, si nécessaire, d´une action en justice spécifique*»[36]. Ainsi, sont reconnus le droit à l´information, le droit d´accès, de rectification, etc.

[Rz 34] Ces droits subjectifs permettent à la personne concernée de maîtriser la circulation de son image informationnelle et d´apprécier les raisons de son utilisation. Cette connaissance lui permettra de faire valoir devant le juge ou l´autorité de protection des données ses libertés[37] et d´opposer celles-ci aux libertés ou à l´intérêt qui fondent le traitement opéré par le responsable du traitement.

[Rz 35] On conçoit à cet égard, le rôle central joué par l´autorité de protection des données dans ce débat entre libertés ou entre libertés et intérêt général. Il s´agit à l´occasion d´un traitement particulier, de mettre en balance les intérêts et libertés mis en cause d´une part et poursuivis d´autre part, afin de déterminer lesquels ou lesquelles doivent prévaloir. Cette mise en balance peut conduire à une remise en cause de l´existence même du traitement ou de manière plus limitée de son contenu.

[Rz 36] La directive de 1995 n´est plus à proprement parler centrée sur la notion de vie privée, conçue comme un noyau dur, condition indispensable des libertés essentielles. C´est désormais tout traitement de données à caractère personnel qui est apprécié à l´aune de l´ensemble des libertés individuelles.

[Rz 37] La directive constitue donc un élargissement de la préoccupation initiale. Elle instaure des droits subjectifs de protection en faveur de la personne concernée[38] et conçoit le débat de la protection des données dans le contexte d´une relation de pouvoirs entre, d´une part, les responsables du traitement et, d´autre part, les personnes concernées.

[Rz 38] Ainsi, c´est à juste titre que la Charte européenne des droits fondamentaux distingue en ses articles 7 et 8 [39] deux concepts qui, certes, peuvent se compléter et se recouper mais dont l´extension n´est pas semblable. L´article 7 évoque dans l´esprit de la Convention de 1950, le respect de la vie privée et familiale du domicile et des communications. L´article 8 énonce le droit à la protection des données à caractère personnel, épingle les limitations au traitement en même temps que les droits subjectifs essentiels de la personne concernée et souligne le rôle de l´autorité indépendante dans le contrôle du respect de ces règles. Cette consécration quasi constitutionnelle de la protection des données comme un principe distinct de celui de la vie privée doit être soulignée. Sans doute, la protection des données s´enracine-t-elle historiquement dans la protection de la vie privée au sens de la Convention européenne des droits de l´ Homme. Sans doute, certains traitements constituent-ils des violations de notre droit à l´ intimité et à notre droit à l´épanouissement mais la réglementation instaurée par cette seconde génération déborde ce cadre étroit et vise d´office en réglementant leur mise en œuvre et leur contenu tout traitement de données à caractère personnel, qu´il y ait ou non atteinte à la vie privée.

[Rz 39] Cette seconde génération qui englobe la directive dite générale de protection des données de même que l´article 8 de la Charte des droits de l´ Homme qui en est le prolongement semble aujourd´hui insuffisante à prendre en compte les risques encourus par les libertés des citoyens du fait des technologies de l´ information et de la communication. On rappellera que la directive de 1995 n´a pu prendre en compte le fait de l´Internet et des nouveaux réseaux numériques, ni d´ailleurs la directive 97/66/CE dite RNIS et vie privée.

[Rz 40] La prise en considération de ces nouveaux réseaux et des utilisations dont on perçoit seulement aujourd´hui les premiers développements amène à devoir considérer un élargissement de la protection des données au-delà des principes mis en place par la directive 95/46/CE.

[Rz 41] Si la technologie de l´ information et de la communication est prise en compte en 1995, son impact est perçu du seul côté du responsable comme un accroissement de leurs pouvoirs et crée dès lors des obligations à la charge de ces derniers de veiller à la sécurité technique et organisationnelle des traitements, la notion de sécurité étant entendue au sens le plus large.

[Rz 42] La révolution que représentent les réseaux numériques pour la protection des données repose sur le fait qu´entre le responsable du traitement tel que conçu par la directive et la personne concernée, la technologie s´interpose à un double titre. Comme nous l´avons montré, elle est à la base de flux conscients ou inconscients provenant du terminal de la personne concernée ou d´un objet qui autorise le contact avec cette personne, même non identifié voire non identifiable. Par ailleurs, le réseau lui-même ne constitue plus, comme c´était le cas dans la communication par circuits, un lien unique entre un émetteur et un destinataire mais autorise un foisonnement de relations non contrôlées où interviennent, à partir de lieux multiples et sans considération de frontières, des intervenants connus ou inconnus.

[Rz 43] Bref, et c´est notre thèse, c´est cette technologie d´interface entre la personne concernée et ces intervenants qu´il importe désormais de réglementer. A notre opinion, la directive 2002/58/CE contient les éléments de base de cette nouvelle approche.

2. Une thèse: la directive 2002/58/CE contient les éléments de base d´une nouvelle approche

[Rz 44] Traditionnellement, la directive de 2002 est considérée comme une application ou spécification[40] des règles contenues dans la directive de 1995 dite directive générale. Elle constitue une révision de la directive sectorielle 97/66/CE du 15 décembre 1997 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications[41] et l´adaptation de cette dernière à l´évolution du marché des technologies et des services de communication et aux risques nouveaux liés à cette évolution.

[Rz 45] Notre propos est de suggérer une autre lecture: l´adoption de la directive de 2002 marque sur certains points limités certes mais importants une rupture avec la conception traditionnelle de la protection de la vie privée, consacrée par la directive 95/46/CE[42]. Notre thèse s´appuie sur le fait qu´ à la fois en ce qui concerne les données protégées, les personnes soumises à des obligations et les objets réglementés, la directive de 2002 déborde le champ d´application de celle de 1995.

[Rz 46] La définition même des **«données»**, dont la protection est au cœur même de la directive récente ne suit pas exactement celle de 1995. Les définitions de «données de trafic» et de «localisation» reprises à l´article 2 évitent soigneusement les expressions de «données à caractère personnel», qui circonscrivent pourtant le champ d´application de la directive 95/46/CE, dont la directive de 2002 ne serait qu´une application. Autant, l´article 2 c) que le considérant 14 de la Directive définissent la donnée de localisation par la seule référence à l´équipement terminal d´un utilisateur. Lorsqu´il s´agit de commenter la notion de donnée de trafic, le considérant 15 parle « *d´informations consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication* ».

[Rz 47] Qu´est-ce à dire? Ces données peuvent ne pas être des données à caractère personnel, en d´autres termes que la recherche du lien avec une personne identifiée ou identifiable n´est plus nécessaire. Sans doute, dira-t-on, l´article 3 à propos des «services concernés» par la directive n´évoque que les «traitements de données à caractère personnel dans le cadre de la fourniture de services de communications dans la Communauté». Dans la mesure où d´autres dispositions de la Directive, comme il sera montré plus loin, réglementent des situations qui excèdent le champ d´application de l´article 3, on n´y prêtera pas nécessairement attention. Il suffit en effet selon la définition de la donnée de trafic ou de localisation qu´un lien puisse être fait avec un terminal, un objet et qu´à travers celui-ci une personne, le possesseur de ce terminal même non identifié puisse soit être atteint, soit être caractérisé pour que cette directive nouvelle s´applique. Une telle conception permettrait demain de réglementer les systèmes d´intelligence ambiante fondées sur des techniques de RFID qui entendent manipuler des données relatives à un objet pour prendre des décisions vis à vis de leurs possesseurs sans s´intéresser à «identifier», au sens classique du terme, ces derniers. En d´autres termes c´est la possibilité, grâce à des données, de prendre des décisions vis à vis de certains individus identifiés ou non, identifiables ou non, qui doit être entourée de garanties

[Rz 48] Prenons, par exemple, un service d´aide à la «navigation touristique» lancé par une commune et fondé sur un réseau d´intelligence ambiante et une technologie RFID. En tant qu´utilisateur de ce système, non obligé de m´identifier, je génère au cours de ma promenade des données de localisation qui me permettent de me repérer et le cas échéant, d´avoir des informations sur les richesses artistiques que je croise. Voilà certes des données de localisation relatives aux utilisateurs visées par l´article 9 de la directive 2002/58/CE. S´agit-il de données à caractère

personnel? Par hypothèse, selon la directive de 1995,non…du moins si aucun lien avec l´identité du porteur du terminal ne peut être fait. On imagine cependant parfaitement l´application de certains articles de la directive 2002/58/CE à de telles données sans caractère personnel: ainsi, l´article 9 en matière d´obligation d´informations du fournisseur de services et en matière de restriction de la durée d´utilisation de ces services et des personnes ayant accès aux données générées. Le même article ne légitimerait le traitement de données que sur base du consentement, celui-ci pouvant être retiré à tout moment (un simple bouton désactivant l´émission d´ondes radio).

[Rz 49] Bref, la directive 2002/58/CE apparaît applicable en dehors des seules données dites à caractère personnel.

[Rz 50] A propos des **personnes assujetties à la directive** 2002/58/CE, on peut comprendre de la même manière la volonté des auteurs de la directive d´éviter soigneusement à propos du fournisseur de services de communication, la notion de «responsables du traitement» au sens de la directive générale. On peut en effet imaginer que le fournisseur d´un service de communication enregistre des données relatives à l´utilisation de terminaux pour lesquels le lien avec l´identité de l´utilisateur soit pratiquement impossible. Ainsi, l´activité de tout fournisseur de service de communication, c´est-à-dire dont l´activité consiste en l´acheminement des données ou des réseaux ou en l´accès à de tels réseaux est réglementée sans nécessairement se fonder sur les règles de la directive générale. Ainsi, les hypothèses de légitimité d´un traitement des données acheminées sont très limitées. Cette restriction s´explique par la nature même de leur intervention, qui est dictée par la seule technologie de communication qui s´impose à tout qui utilise des réseaux.

[Rz 51] Cette situation particulière d´interface explique le rôle que ces fournisseurs peuvent jouer comme «collaborateur» de l´autorité publique dans la recherche d´informations relatives à l´utilisation des réseaux qui pourraient conduire à l´identification de délinquants[43]. Ce rôle, justifie, on le pressent, la mise sur pied de système de cahiers des charges ou d´agrément applicables à ces acteurs d´une nature particulière.

[Rz 52] D´autres dispositions de la directive témoignent bien plus encore de cette approche nouvelle. L´article 5.3 traite de l´utilisation des réseaux de communication en vue de stocker des informations ou d´accéder à des informations stockées dans l´équipement terminal d´un abonné ou d´un utilisateur. L´article 14 évoque lui les caractéristiques techniques et la normalisation des équipements terminaux pour préciser au point 3 que, nonobstant le principe du libre marché, des normes peuvent être imposées à la construction de ces équipements afin de les rendre comparatifs avec le droit des utilisateurs de protéger et contrôler l´utilisation de leurs données à caractère personnel.

[Rz 53] Le rapprochement de ces deux dispositions se justifie par le fait qu´elles concernent toutes deux les **équipements terminaux** et qu´elles constituent des dispositions clairement en dehors du domaine d´application de la directive, domaine fixé comme il a été rappelé par l´article 3.1. de la Directive commentée. Elles ne concernent en effet pas des traitements de données opérées dans le cadre de la fourniture de services de communications électroniques.

[Rz 54] Leur présence est donc d´autant plus significative.

[Rz 55] La première disposition entend prévenir toute intrusion dans l´équipement terminal. On songe aux cookies, aux spywares mais également à des applications plus légitimes permettant par exemple la mise à jour à distance de programmes téléchargés sur l´ordinateur. L´article vise à donner à l´intéressé une maîtrise plus complète de son équipement, en obligeant le responsable de cette intrusion (le responsable du traitement des données)[44] à donner certaines informations à l´utilisateur du terminal sur la finalité de l´intrusion et à lui permettre de refuser cette dernière.

[Rz 56] L´article 14[45] de la directive 2002/58/CE prolonge cette première disposition relative au terminal. Dans la mesure où ce sont les spécifications techniques de fonctionnement du terminal qui permettent ces intrusions ou de manière plus générale certaines atteintes à la protection des données, la Commission se réserve le droit d´imposer aux fabricants d´équipements certaines normes qui assurent la compatibilité du terminal avec le respect des exigences de protection des données.

3. Conclusions de l´ acte II

[Rz 57] Notre propos était de montrer l´attention que la directive 2002/58/CE donne, au-delà des questions traditionnelles de protection des données à caractère personnel, au fait technologique que représente le fonctionnement des réseaux, indépendamment des rapports entre la personne concernée et les responsables de traitement.

[Rz 58] Ainsi, la directive permet l´extension de la protection à des catégories de données qui ne sont point nécessairement qualifiables de données à caractère personnel dans la mesure où elles sont liées à des terminaux et non à des personnes.

[Rz 59] Ainsi, la directive 2002/58/CE dite «vie privée et communications électroniques» pointe le rôle particulier de deux acteurs, indépendamment de leur qualité de responsables de traitement:

- Les opérateurs de réseaux (en ce compris les fournisseurs d´accès à Internet), c´est-à-dire ceux qui fournissent «des systèmes de transmission et le cas échéant, les équipements de communication ou de routage et les autres ressources qui permettent l´acheminement de signaux[46]» qui constituent des interfaces obligés entre l´utilisateur du réseau en tant que personne concernée et les multiples acteurs de l´Internet qui pourront traiter les données multiples générées consciemment ou non par l´utilisation du réseau. C´est à eux qu´incombent certains devoirs, tels celui de prévenir des risques liées à l´utilisation du réseau, de garantir la sécurité de ses services, de permettre des restrictions à l´identification de la ligne appelante, etc.;
- les fournisseurs d´équipements terminaux, en particulier -mais non uniquement-, des logiciels de navigation, dont les caractéristiques techniques doivent mettre en œuvre les dispositions de la directive. En particulier, la Directive prévoit la possibilité d´imposer certaines «mesures afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l´utilisation de leurs données à caractère personnel».

[Rz 60] Cette extension doit se concevoir comme un complément des deux premières approches. Comme il a été montré, la deuxième approche signifiait déjà une rupture avec la première dans la mesure où la notion de vie privée, préoccupation à l´origine des lois de protection des données, s´est effacée au profit d´un régime général de protection des données à caractère personnel et par l´octroi de droits subjectifs aux personnes concernées et d´obligations précises pour les responsables de traitement. La troisième approche ne remet pas en cause ces deux premières approches. Au contraire, elle s´ y enracine mais la prise en compte les risques nouveaux liées aux réseaux de communication électronique conduit à un nouvel élargissement de la protection des libertés des citoyens.

III. Acte III: Où il est question de nouveaux principes de protection des données permettant d´assurer aux personnes une protection adéquate dans l´environnement des réseaux modernes de communications électroniques

[Rz 61] Les caractéristiques de l´environnement des services de communication électronique (omniprésence, complexité, opacité, performance et polyvalence) et des terminaux (interactivité, dimension internationale des réseaux et services et producteurs d´équipement, opacité de fonctionnement) créent de nouveaux risques et aggravent les risques d´atteinte aux libertés individuelles et à la dignité humaine.

[Rz 62] La parade à ces risques n´est possible que par la consécration de principes nouveaux améliorant la protection des individus et lui donnant une meilleure maîtrise de leur environnement. Ce n´est en effet que dans la mesure où cette maîtrise est possible, que la personne concernée pourra prendre effectivement la responsabilité de sa propre protection et mieux disposer des moyens d´une véritable autodétermination informationnelle.

[Rz 63] La formulation de ces nouveaux principes est une première tentative de ce qui pourrait, au-delà des prescrits de la directive 2002/58/CE que nous venons d´analyser, constituer les bases d´une troisième génération de législation de protection des données.

1. Premier principe: Du chiffrement et de l´anonymat «réversible»

[Rz 64] Le chiffrement des messages assure la protection de l´accès au contenu des communications. Leur qualité varie et les techniques de chiffrement et de déchiffrement peuvent également être diverses. Les logiciels d´encryptage placés sur l´ordinateur de l´internaute (par exemple, SSL ou PGP) sont désormais accessibles à des prix abordables et généralement intégrés dans les logiciels grand public. La notion d´anonymat quant à elle devrait sans doute être redéfinie et, dans la foulée, d´autres termes comme «pseudonyme» ou «non identifiabilité» devraient être préférés dans la mesure où cette notion d´anonymat demeure ambiguë. Ce qui est recherché est bien souvent, non un anonymat absolu, mais une «*non identifiabilité» fonctionnelle de l´auteur d´un message vis-à-vis de certaines personnes*[47]. Nombre de textes à caractère non contraignant préconisent le «droit» du citoyen[48] à disposer de l´anonymat lorsqu´il utilise les services offerts par les technologies nouvelles. La Recommandation n° R(99) 5 du Comité des Ministres du Conseil de l´Europe[49] énonce, nous le rappelons, le même principe: «*L´accès et l´utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée* .» et souligne à ce propos l´intérêt des «Privacy Enhancing Technologies» disponibles sur le marché. Au-delà, on connaît les prescrits de la directive 2002/58/CE qui permettent à l´utilisateur d´un terminal téléphonique[50] d´ éviter la présentation de la ligne appelante et de la ligne connectée. L´article 9.2. de la même directive rend obligatoire la possibilité, pour l´ utilisateur d´ un terminal permettant la géo-localisation et qui ne s´est point opposé au départ à cette possibilité, d´interdire temporairement le traitement de ces données pour chaque connexion ou pour chaque transmission de communication.

[Rz 65] En d´autres termes, celui qui utilise les moyens modernes de communication devrait avoir le choix de rester non identifiable au regard, tantôt de tiers intervenant dans l´acheminement du message ou de prestataires intervenant dans cette chaîne de communication, tantôt du ou des destinataires de la communication et disposer gratuitement, ou au moins à des prix abordables, des moyens d´exercer son choix[51]. La mise à disposition à des coûts abordables de moyens ou de services de chiffrement et d´anonymisation est une condition nécessaire à une responsabilisation de l´internaute.

[Rz 66] L´anonymat ou la «non identifiabilité fonctionnelle» requis ne sont cependant pas absolus. Au droit à l´anonymat des citoyens, s´oppose l´intérêt supérieur de l´Etat qui pourra imposer des limitations lorsque celles-ci constituent des mesures nécessaires «*pour sauvegarder la sûreté de l´Etat, la défense, la sécurité publique la prévention, la recherche, la détection et la poursuite de (certaines) infractions pénales* ». L´équilibre entre le légitime contrôle des infractions et la protection des données pourrait être trouvé dans des systèmes de «pseudo-identité» attribuée à un individu par un fournisseur de service spécialisé auprès duquel dans les seuls cas prévus par la loi et moyennant les modalités fixées par celle-ci pourrait s´opérer le lien entre l´identité réelle d´un usage et son pseudonyme.

[Rz 67] Au-delà, d´autres solutions pourraient être imposées par une réglementation des appareils terminaux: suppression du «bavardage» des navigateurs, la création d´adresses éphémères ou relatives à un groupe d´individus et une différenciation des données d´adressage suivant les tiers qui auront accès aux données de trafic ou de localisation et la disparition des pointeurs (Global Unique Identifiers) par l´uniformisation des protocoles d´adressage.

[Rz 68] Nos réflexions sur les terminaux identifiant des objets à défaut des personnes qui les possèdent amènent à élargir le propos. Ne peut-on considérer que c´est un droit pour l´utilisateur d´un tel terminal de supprimer le fonctionnement de ce terminal: ainsi la personne promenant son caddie dans une grande surface fonctionnant comme un système d´intelligence ambiante, a le droit de désactiver à tout moment le RFID qui permet de contrôler ses mouvements voire de les guider[52].

[Rz 69] Dernière remarque: le statut des «anonymisers», véritable tiers de confiance pour celui qui y fait appel, devrait être réglementé afin d´offrir, d´une part, à celui qui y recourt certaines garanties quant à la qualité des services offerts et, d´autre part, à l´Etat, la garantie de pouvoir techniquement accéder au contenu des télécommunications, dans les conditions prévues par la loi[53].

2. Deuxième principe: La réciprocité des avantages:

[Rz 70] Ce principe pourrait s´exprimer comme suit: le législateur met à charge de celui qui utilise la technologie aux fins de développer ses activités professionnelles, certaines obligations supplémentaires qui permettent de rétablir l´équilibre traditionnel des parties en présence. La justification du principe est simple, si la technologie accroît les

capacités de collecte de traitement, de communication des informations relatives à autrui, si la technologie facilite la conclusion de transactions ou d´opérations administratives, il est indispensable que cette même technologie soit configurée et utilisée de manière telle que la personne concernée, l´administré, le consommateur, bref le fiché, puisse bénéficier, dans une proportion comparable, des avantages de cette technologie.

[Rz 71] Quelques dispositions récentes se fondent sur l´exigence de la réciprocité des avantages pour obliger celui qui utilise des technologies à mettre à disposition de l´internaute des moyens électroniques pour faire valoir ses intérêts ou ses droits qui peuvent être mis à mal par l´utilisation de ces moyens électroniques.

[Rz 72] Les exemples législatifs tirés des directives européennes récentes ne manquent pas. Ainsi, premier exemple, la directive européenne 2001/31/CE sur les services de la société de l´information prévoit la possibilité de s´opposer *via des moyens électroniques* au spamming. En d´autres termes, celui qui utilise pour diffuser de manière plus efficace et rapide ses messages publicitaires les technologies de l´information et de la communication doit accepter que le destinataire utilise les mêmes voies pour s´opposer à toute diffusion ultérieure. Deuxième exemple déjà cité, l´article 5.3 de la directive 2002/58 «Vie privée et communications électroniques» exige de même que toute « *utilisation des réseaux de communications électroniques en vue de stocker des informations ou d´accéder à des informations stockées dans l´équipement terminal d´un abonné ou utilisateur faire l´objet d´une information de ce dernier et que celui-ci dispose du droit de refuser un tel traitement* …». les commentateurs insistent sur le fait qu´un tel refus doit pouvoir s´exprimer par un moyen aisé, un simple clic à partir du terminal et non l´utilisation d´une correspondance écrite. Enfin, troisième exemple: la possibilité pour l´abonné (article 8.1. de la directive 2002/58/CE) de restreindre «*par un moyen simple et gratuit l´identification de la ligne appelante et ce, appel par appel…et ce, pour chaque ligne* » est une autre manifestation, riche d´applications possibles si l´on veut bien suivre le raisonnement proposé dans le premier principe. Cette possibilité de restriction d´identification de la ligne appelante conduit à une obligation corrélative pour le fournisseur du service de permettre, *par un moyen simple et gratuit, poursuit la directive,* au destinataire soit de refuser les appels entrants non identifiés, soit d´empêcher leur identification (article 8.2 et 8.3).

[Rz 73] Au-delà, dans le cadre des réseaux de communication électroniques, on peut de même envisager que certains droits de la personne concernée, ainsi le droit à l´information, le droit d´accès et de rectification et le droit de recours puissent demain se réaliser par des moyens électroniques que permet le fonctionnement interactif du réseau. De multiples applications de ce droit peuvent dès maintenant être suggérées.

- Le **droit à l´information** de la personne concernée doit pouvoir s´opérer à tout moment par un simple clic (ou plus largement par un simple geste positif, électronique et immédiat) sur un sigle permettant l´accès à une «Privacy Policy» dont on peut espérer qu´elle soit d´autant plus précise et complète que le coût de la diffusion est réduit dans le cas de l´utilisation du média électronique. Cette démarche doit rester anonyme pour le serveur de la page (crainte de «fichage» des internautes «privacy concerned»). Au-delà, en cas de labellisation du site, on peut songer à rendre obligatoire l´existence d´un hyperlien qui permettrait à partir du sigle du label de visiter la page du site de l´organe de labellisation relative au site web en question. Même suggestion à propos de la déclaration d´un maître du fichier à l´autorité de contrôle, un hyperlien serait ainsi placé sur une page incontournable du site web, objet du traitement déclaré et la page du site de l´autorité de contrôle reprenant la déclaration du site concerné.

- Le **droit d´accès** de la personne concernée doit demain pouvoir s´exercer via le média électronique sur base de l´utilisation de la signature électronique. Il devrait obliger la personne responsable à structurer ses fichiers de manière à permettre à la personne d´exercer de façon aisée ce droit d´accès. Des renseignements complémentaires comme l´origine des données, la liste des tiers à qui communication de certaines données a été faite devraient être systématiques.

- Au-delà, notons que dans les vastes réseaux publics et privés, la donnée à caractère personnel n´est plus collectée pour une ou des finalités précises mais «déposée» à un endroit du réseau pour servir à des finalités définies de manière évolutive en fonction des capacités de traitement nouvelles ou de besoins non aperçus au départ. Face à cette réalité, il importe que la personne concernée puisse obtenir une documentation décrivant les flux au sein du réseau, les données en question et les divers utilisateurs, bref ce qu´on peut appeler un « **cadastre des flux**»[54].

- les **droits de rectification et/ou d´opposition** devraient pouvoir s´opposer en ligne auprès d´une personne désignée chargée de l´examen de plaintes ou de gérer la liste des oppositions, acteur dont le statut devrait être défini.

- le **droit de recours**, également, ne mériterait-il pas de pouvoir bénéficier des avantages que représente la cybermagistrature, saisine on-line, gestion de l´échange par voie électronique des arguments des deux parties et finalement prononcé de la décision ou de la proposition de médiation?

- le droit lorsqu´une décision soit automatisée, soit signifiée par le biais d´un réseau est opposée à la personne concernée (ainsi, refus d´un permis de bâtir suite à une procédure dite de télé-administration) de pouvoir connaître par le même canal la logique suivie pour la prise de décision. A cet égard, en matière de service public[55], le citoyen devrait pouvoir bénéficier du droit de pouvoir tester de manière anonyme les logiciels d´aide à la décision ou systèmes expert qui pourront lui être appliqués le cas échéant (ainsi, un logiciel d´aide au calcul automatique des impôts ou des primes susceptibles d´être obtenues en matière de réhabilitation d´un logement).

3. Troisième principe: La promotion de solutions technologiques conformes au respect des principes de protection des données ou améliorant la situation des personnes protégées par le droit

[Rz 74] La Recommandation 1/99 du 23 février 1999[56], émise par le Groupe dit de l´article 29 sur base d´une analyse des risques créés pour la vie privée par les logiciels et matériels utilisés pour la communication via Internet, émet le principe suivant lequel l´industrie du logiciel et du matériel se devait de développer des produits en conformité avec les dispositions des directives en matière de protection des données personnelles. Ce troisième principe répété dans d´autres avis du groupe dit de l´article 29[57] conduit à reconnaître aux régulateurs diverses modalités d´intervention.

[Rz 75] Ainsi, il s´agit pour lui de pouvoir intervenir en cas de développements technologiques présentant des risques majeurs. Ce **principe dit de «précaution»** largement connu en droit de l´environnement[58] pourrait trouver à s´appliquer en matière de protection des données. Au nom de ce principe de précaution, il apparaît d´ailleurs comme nécessaire que les équipements terminaux de télécommunication (en ce compris les logiciels qui les animent) adoptent le paramétrage par défaut le plus protecteur possible, de manière à ce que la personne concernée ne puisse pas, par défaut, être exposée à divers risques qu´elle ignore ou qu´elle ne sait mesurer.

[Rz 76] Par ailleurs, au nom de **principe de réciprocité des avantages**, il paraît opportun et non déraisonnable de doter certains équipements terminaux de télécommunications, de «journaux de bord», à l´instar de ce qui se fait pour les logiciels de type «serveur» déployés par les entreprises et les administrations en ligne. Ceci permettrait à chaque utilisateur d´apprécier et de contrôler les personnes qui ont eu accès à son équipement et, le cas échéant, de visualiser les caractéristiques essentielles des transferts d´information entrants et sortants.

[Rz 77] Une disposition de la directive européenne «vie privée et communications électroniques» déjà citée, pourrait servir de base à cette obligation mise à charge des fabricants de terminaux. L´article 14 prévoit qu´en cas de non conformité d´un équipement terminal aux règles de protection des données, la Commission peut prendre des initiatives en matière de standardisation de ceux-ci. En d´autres termes, la normalisation technique des équipements terminaux constitue une mesure – certes subsidiaire – d´assurer la protection des données à caractère personnel contre les risques de certains traitements abusifs, risques créés par les choix technologiques.

[Rz 78] Au-delà, au nom du principe de sécurité, prescrit par l´article 7 de la Convention n°108 du Conseil de l´Europe, il s´agit d´interdire les «**Privacy Killing Technologies**»[59]. L´obligation de prévoir des mesures techniques et organisationnelles appropriées aux risques engendrés pour la protection des données conduira le responsable d´un site à veiller à la confidentialité des messages échangés, à signaler clairement les transmissions de données - fussent-elles automatiques et par hyperlien comme c´est le cas avec les sociétés de cybermarketing - et à lui donner les moyens aisés de les bloquer.

[Rz 79] Cette même obligation de sécurité a pour conséquence d´imposer à celui qui développe des terminaux, le choix de solutions technologiques aptes à minimiser voire à réduire à néant les risques d´atteinte à la vie privée.

L´influence de ce prescrit sur le design des cartes à puce en particulier les cartes multifonctionnelles[60], comme les cartes d´identité, est évident.

[Rz 80] Peut-on aller plus loin et recommander le développement de «Privacy Enhancing Technologies», c´est-à-dire d´outils ou de systèmes qui permettent de mieux assurer le respect des droits de la personne concernée[61]? Il est certain que c´est le marché qui, librement, développera ces technologies mais la promotion de telles solutions «privacy compliant» ou «privacy enhancing» exige un rôle actif de l´Etat, celui de veiller par des subsides à la recherche et au développement de ces solutions; celui de mise en place de systèmes volontaires de certification ou d´accréditation des solutions élaborées et d´assurer la publicité de ces «labels»; celui, enfin, de mettre à disposition à des coûts «abordables» les solutions technologiques considérées comme nécessaires à la protection des données[62].

[Rz 81] Quatrième principe: La maîtrise par l´utilisateur du fonctionnement des équipements terminaux

[Rz 82] La justification du principe est évidente. Dans la mesure où ces terminaux permettent à autrui de capter nos comportements, nos actions ou simplement de nous localiser, leur fonctionnement doit être transparent et sous notre contrôle. L´article 5.3. de la directive 2002/58/CE déjà citée en est une première illustration. La personne doit être clairement informée de toute utilisation à distance de son terminal (cookies, spyware) et pouvoir facilement et gratuitement s´y opposer. La règle posée par la directive 2002/58/CE qui permet à l´utilisateur d´une ligne appelante ou connectée de pouvoir empêcher la présentation de l´identification de la ligne appelante ou appelée constitue une autre illustration du principe.

[Rz 83] Au-delà de ces exemples, on pose **le principe que tout équipement terminal devrait être paramétré de telle manière que son possesseur ou utilisateur puisse être informé de manière complète des flux entrants et sortants et puisse agir en connaissance de cause, s´il l´estime nécessaire.**

[Rz 84] De même, la possession d´une carte à puce devrait être accompagnée, comme le prévoient certaines législations sur les cartes d´identité électronique d´une possibilité d´accès en lecture des données inscrites sur la carte, par la personne concernée. La maîtrise suppose également, nous l´avons dit, que la personne puisse à tout moment décider de désactiver définitivement le terminal. En matière de RFID, la question est importante. La personne concernée doit pouvoir, gratuitement et facilement, auprès de tiers fiables[63] s´assurer de la désactivation de ce moyen technique de repérage à distance.

[Rz 85] On note que l´usager devra pouvoir opposer ce principe à des entreprises non nécessairement visées par les réglementations classiques de protection des données dans la mesure où elles ne sont point responsables de traitement: ainsi les fournisseurs d´équipements terminaux et des multiples logiciels en particulier de navigation susceptibles d´être incorporés au terminal pour faciliter la réception, le traitement ou l´émission de communications électroniques.

[Rz 86] Au-delà, il s´adresse aux organes de normalisation tant publics que privés qui s´occupent ou se préoccupent de la configuration de ces équipements.

[Rz 87] **L´idée essentielle est que les produits mis à la disposition des usagers des services de communications électroniques ne puissent permettre de par leur configuration même des agissements illicites, qu´ils soient le fait de tiers ou du producteur lui-même**.

[Rz 88] Quelques exemples illustrent l´importance du propos:

- la comparaison des navigateurs présents sur le marché démontre que le bavardage de certains d´entre eux va bien au-delà de ce qui est strictement nécessaire à l´établissement de la communication[64];

- le traitement de la réception, de la suppression et du blocage d´envoi des cookies diffère d´un navigateur à l´autre. Ainsi, suivant les programmes de navigation et leur configuration, des traitements déloyaux seront plus ou moins faciles; le blocage des fenêtre «pop-up» ou de l´envoi systématique des références des articles lus en ligne ou des mots-clés frappés sur les moteurs de recherche ne semble tout simplement pas possible ou, en tous cas, pas possible de manière simple sur le navigateur installé par défaut sur la plupart des centaines de millions

d´ordinateurs personnels;

- l´utilisation d´identifiants globaux uniques (GUID)» ou de logiciels espions est également à signaler.

[Rz 89] Par ailleurs, on s´interroge sur la nécessité d´équipements terminaux transparents dans leur fonctionnement permettant à leur usager d´avoir la pleine maîtrise des données envoyées et reçues. Ainsi, l´usager devrait pouvoir connaître de manière conviviale l´étendue exacte du bavardage de son ordinateur, les informations transmises et reçues, leur finalité et leur émetteur ou leur destinataire. A cette fin le journal de bord apparaît comme une technique appropriée et relativement aisée à mettre en œuvre.

[Rz 90] Au-delà de ce droit de l´utilisateur d´être informé des flux entrants, on peut s´interroger sur le droit de la personne de soumettre à autorisation le fait pour un tiers de pénétrer son «domicile virtuel». Il convient ici de rappeler les dispositions de la Convention du Conseil de l´Europe concernant la Cybercriminalité et notamment ses articles 2[65] (accès illégal) et 3[66] (Interception illégale).

[Rz 91] On remarquera ici que l´identification ou l´identifiabilité des personnes participant à une télécommunication ne constitue pas une condition d´application de cette Convention. Semblablement, l´accès non autorisé à un système informatique ne se limite pas au hacking de gros systèmes informatiques appartenant à des banques ou à des administrations mais concerne aussi l´accès non autorisé à un terminal de télécommunication qui, en l´état actuel de l´art, est un ordinateur[67] et ce indépendamment de toute infraction aux lois protégeant les données à caractère personnel. L´ intrusion dans un terminal est en soi une infraction[68].

IV. Conclusions finales[69]

[Rz 92] Le contexte de l´Internet appelle une troisième génération de réglementations en matière de protection des données. Il ne s´agit pas de tourner le dos aux deux premières générations mais d´ajouter à celles-ci tout en ne modifiant pas les options déjà prises un niveau supplémentaire de protection. La première génération était essentiellement caractérisée par une approche fondée sur la nature de la donnée: était-elle sensible? Appartenait-elle à la sphère intime de la personne concernée? L´autodétermination informationnelle est alors comprise comme l´interdiction de traiter certaines données. C´est l´époque de la consécration de l´article 8 de la Convention européenne des droits de l´Homme. La deuxième génération ajoute à la première la nécessité, au-delà de la protection de ces données particulières, d´envisager la façon dont le traitement de données à caractère personnel peut modifier les relations de pouvoir entre celui qui traite les données et celui à propos duquel le traitement a lieu. L´autodétermination informationnelle s´entend alors de la nécessité de rééquilibrer la relation en garantissant la transparence des traitements et en limitant le droit de traiter les données d´autrui. La Convention n° 108 est née dans cet esprit. Elle a fait de nombreuses émules et démontré ainsi amplement son bien-fondé.

[Rz 93] **Ce qui caractérise la troisième génération que nous voyons poindre et dont nous souhaitons la consécration rapide est la prise en compte du fait technologique en lui-même** . Que l´utilisation de la technologie multiplie les données et les personnes capables d´y accéder, qu´elle accroît la puissance de ceux qui, grâce à elle, peuvent les collecter et mieux les traiter, qu´elle abolisse les frontières est un premier constat. La complexité du fait technologique, son opacité constituent une seconde réalité à prendre en compte. Entre la personne concernée et les maîtres du fichier s´invite une troisième personnage tour à tour «terminal» et «réseau». L´autodétermination informationnelle passe dorénavant par une maîtrise de ce troisième personnage.

[Rz 94] Comment envisager cette maîtrise? Nous présentons ci-après quelques pistes de réflexion sans prétendre épuiser le sujet. La première concerne la façon d´ y répondre. “The answer to the machine is in the machine»: cette affirmation, lancée par C. Clarke[70] à propos des problèmes rencontrés par la protection des droits d´auteur dans la société de l´information, peut servir de guide pour trouver une réponse adéquate aux risques encourus par la vie privée du fait de la société de l´information. Ainsi, nous avons vu que le principe de réciprocité des avantages, la promotion de solutions technologiques «Privacy Minded» peuvent favoriser une meilleure maîtrise par la personne concernée de la circulation et de l´utilisation de son image informationnelle.

[Rz 95] Cet optimisme a des limites: si les technologies peuvent renforcer ce que certains appellent l´«User

Empowerment», c´est au risque de laisser seule la personne concernée face au(x) maîtres du fichier. Ce risque est d´autant plus réel que le développement de la technologie n´est pas neutre: si la technologie de l´internet demeure largement «offerte» aux citoyens, son développement est financé de manière indirecte par les entreprises et les administrations qui paient les ordinateurs serveurs. De manière inéluctable, son développement penche donc tout naturellement du côté des intérêts des ficheurs plutôt que vers la défense des fichés. La technologie dite de protection de la vie privée transforme ou risque de transformer la relation de l´individu à la donnée qui le concerne en une relation de propriété que la technologie permet de négocier. C´est le lieu de rappeler que l´autodétermination informationnelle est une liberté qui ne peut totalement se négocier et que c´est le devoir de la société de fixer certaines limites au droit de disposer de ces données.

[Rz 96] Cette focalisation sur les outils technologiques doit amener à la prise en considération de nouveaux acteurs, non aperçus par les législations de deuxième génération: ainsi les fournisseurs de services de communication et les fournisseurs d´équipements terminaux. Leur rôle est décisif si on souhaite que l´utilisateur des services nouveaux de la société de l´information puisse contrôler les flux entrants et sortants de même que les traces laissées au fil des réseaux et leur possible utilisation. La responsabilité objective dans la fourniture d´équipements ou de services «privacy compliant» doit être envisagée.

[Rz 97] Ainsi, en premier lieu, les fournisseurs d´accès à Internet, les opérateurs de mobilophonie ou de téléphonie se voient confiés la charge de sensibiliser le public sur les risques encourus lors de l´utilisation de leurs réseaux, de dénoncer les technologies «privacides» et, en même temps, de fournir un accès à des technologies «privaphiles» appropriées. Le rôle de ces fournisseurs d´accès est essentiel dans la mesure où ceux-ci représentent le point de passage obligé entre l´internaute et le réseau. Ainsi, leur demandera-t-on[71], d´«informer l´internaute des moyens techniques qu´il peut utiliser licitement pour diminuer les risques concernant la sécurité des données et des communications», d´utiliser les procédures appropriées et les technologies disponibles, de préférence celles faisant l´objet d´une certification, garantissant la vie privée et notamment l´intégrité et la confidentialité des données ainsi que la sécurité physique et logique du réseau…», «d´informer ces derniers (les internautes) des moyens d´utiliser ses services et de les payer anonymement». Il offrira à ses abonnés une hotline leur permettant de dénoncer des violations de la vie privée et souscrira à un code de conduite suivant lequel il bloquera l´accès aux sites qui ne respectent pas les exigences posées en matière de protection des données et ce, peu importe la localisation du site.

[Rz 98] En second lieu, on vise les constructeurs et développeurs des matériels et logiciels qui conçoivent et construisent les équipements terminaux, ainsi que les responsables de l´élaboration des protocoles et des standards techniques utilisés pour transmettre des informations en réseau. Ils veilleront à concevoir des produits ou normes[72]:

- conformes, au cadre légal, par exemple par la transmission par les navigateurs internet des informations minimales nécessaires à la connexion ou par l´adoption de mesures de sécurité adéquates;

- qui facilitent l´application des principes dégagés ci-dessus au titre II et qui permettent par exemple un accès direct par l´utilisateur à ses données personnelles ou un droit d´opposition automatique, notamment par le biais de journaux de bord;

- et qui améliorent le niveau de protection des données à caractère personnel.

[Rz 99] L´outil technologique permet de plus en plus de traiter les données relatives à la personne concernée non point, comme c´était le cas de manière classique, par ses données d´identité légale (nom prénom, résidence, etc.) mais par un point d´ancrage voire par un objet (l´intelligence dite ambiante) qui lui est associé. Au-delà, le danger n´est souvent plus dans la collecte *a priori* de données sur l´individu mais sur l´application *a posteriori* à un individu d´un profil abstrait…

[Rz 100] Le terminal, conçu au sens large, doit être traité comme un outil technologique totalement transparent pour celui qui en est le détenteur et l´utilise. Mieux, dans de nombreux cas, il appartient à la personne concernée et pourrait être assimilé à son domicile, c´est-à-dire au lieu où la personne se sent chez elle. L´intrusion dans ce domicile privé doit être traitée comme toute autre intrusion.

[Rz 101] L´opacité et la complexité des systèmes complexes d´informations auxquels les personnes concernées

confient leurs données obligent à un surcroît d´informations non plus centrées sur le ou les traitements eux-mêmes pris séparément et sur leurs caractéristiques mais sur le fonctionnement global du système d´informations en tant que capable de générer une multitude de traitements présents ou à venir: ainsi, l´obligation de documenter les données (origine, utilisateurs, logique de raisonnement), d´établir un descriptif des circuits d´information) et de fixer les règles par lesquelles les décisions sont prises, les règles d´accès définies et contrôlées, etc .

[Rz 102] La prise en considération de l´outil technologique a jusqu´ à présent peu été le fait de ceux qui ont à garantir la protection des données: les autorités de protection des données disposent rarement d´une équipe d´informaticiens à même de décrypter les dangers des innovations technologiques. Sans doute serait-il utile de créer à l´ échelon européen une «Privacy Technology Task Force» permanente, qui pourrait procéder à un technology assessment des technologies mouvelles émergentes. Par ailleurs, les autorités de protection des données se doivent de pénétrer les cénacles où se décident les évolutions technologiques et de la configuration des produits. Ainsi, le dialogue avec les organes de standardisation devrait être créé [73] et sans doute au-delà, sans doute faudrait-il que le Governmental Advisory Committee (GAC) créé à l´ initiative européenne auprès de l´ICANN, autorité privée qui décide de la gouvernance de l´Internet en matière d´adresses et de noms de domaines se penche sur la question de la protection des données. On peut suggérer voire imposer la création d´un Data Protection Advisory Committee auprès de l´ICANN, du W3C et de l´IETF?

[Rz 103] La sensibilisation du milieu sectoriel de la communication électronique aux enjeux de protection des données s´avère en tout cas nécessaire.

[Rz 104] En conclusion, les diverses pistes proposées à la discussion du Comité consultatif ont pour objectifs:

- de mettre à la disposition de l´individu tout ce qui est nécessaire pour comprendre et maîtriser son environnement informationnel en particulier celui qui pénètre son foyer. Il lui donne la maîtrise des outils dont l´utilisation le révèle à autrui;

- de confier à la société les outils lui permettant de pouvoir continuer à maîtriser un développement technologique, dont l´enjeu est bien la survie de nos libertés tant individuelles que collectives.

[Rz 105] Sur le réseau routier, la législation a imposé certaine règles à ses usagers afin, non seulement d´éviter des accidents, mais bien aussi de régler de manière équitable les droits et obligations réciproques des différents usagers de la route, avec en général, une propension prétorienne à protéger tout naturellement l´usager le plus faible. Pour ce faire, au-delà du code de la route, est apparue la nécessité d´une intervention législative toute particulière afin de réglementer le réseau routier lui-même ainsi que les véhicules qui sont admis à y circuler, moyennant le respect de certaines normes obligatoires.

[Rz 106] Sur les autoroutes de l´information, il n´existe aucune législation qui s´attache à définir des normes de fonctionnement des télécommunications respectueuses de la protection de la vie privée des internautes ou encore des exigences de fonctionnement loyal et transparent des terminaux de télécommunication permettant aux internautes de circuler sur ces autoroutes.

[Rz 107] Ce n´est pourtant qu´en appliquant les principes classiques de la protection des données à la technologie, ce troisième larron qui s´invite de manière implicite mais certaine dans toute télécommunication, que l´informatisation de la société pourra conduire à une société de l´information démocratique, moteur de progrès partout et pour tous.

Yves POULLET, Ph.D. in Law and graduated in Philosophy, is professor at the Faculty of Law at the University of Namur and Liège, Belgium (FUNDP & Ulg), Dean of the Faculty of Law in Namur.

1

Pour un historique des RFID, voir: www.rfidjournal.com/article/articleview/1338/1/129 et les questions vie privée liées à ces applications nouvelles, S.E. Sarma,S.A.Weis and D.W.Engels, «*RFID Systems and Security and privacy Implications*», Auto-Id Center MIT, Cambridge, disponible sur www.autoidcenter.org

2 «*L´environnement d´intelligence ambiante sera capable de reconnaître et de réagir à la présence d´individus et fonctionnera de manière fluide et imperceptible, voire souvent totalement non transparente…* », IPTS, «sécurité et respect de la vie privée du citoyen à l´ heure du numérique après le 11 septembre», Doc. de synthèse, juillet 2003, disponible sur le site de la Commission: http://europa.eu.int/comm/justice_home/fsj/privacy/

3 A suivre le cas Baja Beach Club, discothèque barcelonaise où le contrôle d´entrée, le calcul des consommations et les déplacements des membres du clubs sont contrôlés par un système de RFID fonctionnant grâce à un implant Verichips (www.bajabeach.es)..

4 Sur la «nanotechnologie» et ses progrès, on consultera pour la définition: www.techweb.com/encyclopedia,

5 A cet égard, le projet de loi annoncé aux Etats Unis qui viserait à implanter dans le corps de chaque citoyen américain un RFID qui permettrait de connaître les données essentielles de santé en cas d´intervention d´urgence. Les capsules RFID seraient liées à une base de données informatisée créée par le département (= ministère) de la santé des USA afin de stocker et de contrôler les registres de santé de la nation. Cela pourrait être le précurseur d´un projet semblable au Royaume-Uni.
www.pcinpact.com/actu/news/RFID_projet_de_loi_un_implant_pour_chaque_citoyen.htm

6 Y.Poullet et J.M. Dinant, «*L´autodétermination informationnelle à l´ ère de l´ Internet*», Eléments de réflexion sur la Convention n° 108 destiné au travail futur du Comité consultatif (T-PD), Rapport en voie de publication, Novembre 2004).

7 Calcul réalisé sur base d´une extrapolation des chiffres fournis par l´Union Internationale des Télécommunications pour l´année 1999 (vu sur: http: //www.itu.int/ITU-D/ict/statistics/at glance/Eurostat 2001.pdf).

8 En 1980, cela eut nécessité au bas mot des millions d´enregistreurs avec autant de bandes magnétiques. A cette époque, il fallait un enregistreur pour enregistrer une conversation.

9 Voir, par exemple sur www.hitachi.com le 400GB Deskstar 7K400.

10 Actuellement, des débits de 2,5 à 10 gigabits par seconde sont classiques sur ce type de support.

11 Soit environ 2 milliards d´octets.

12 Directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, JOCE n° L 091 du 07/04/1999 pp. 0010 – 0028

13 Ces terminaux que sont les RFID possèdent les éléments suivants:
[Aufzählung]
un processeur;
une mémoire morte;
une antenne qui permet tout à la fois de communiquer avec un terminal et de recevoir l´énergie requise pour faire fonctionner l´ordinateur;
absence de périphériques d´entrée/sortie accessibles à un être humain;
très haut degré de miniaturisation (de l´ordre de quelques millimètres, antenne incluse) Sur les RFID, le lecteur consultera le site très complet: http: //www.rfida.com/nb/identity.htm.

14 Certaines cartes à puces sont équipées de processeurs aussi puissants que les célèbres Apple du début des années 80.

15

Le marché des RFID´s se déploie à une échelle mondiale pour identifier et tracer la plupart des biens matériels. On a cité comme cas les chemises Beneton ou les rasoirs Gilette. Les arguments généralement avancés sont la lutte contre le vol en magasin et un environnement ambiant plus intelligent qui permettraient aux objets même les plus insignifiants de communiquer avec leur utilisateur. Une autre utilisation possible est constituée par le numéro de série qui pourrait être gravé dans cette puce scellée dans l´objet. Le système de codification des RFID est révélateur de son ambition. Le code EAN (European Article Number) se compose de 96 bits dont les 36 derniers sont réservés pour le seul numéro de série de l´article. Il s´agit donc de permettre l´identification individuelle de 16 milliards d´objets identiques (du même type et produits par la même firme). Si on ne voit pas quelle entreprise pourrait produire 16 milliards de produits identifiques ni l´utilité de différencier le cas échéant ces milliards d´objets identiques, on notera qu´il s´agit de l´ordre de grandeur de la taille prévisible de la population mondiale dans les décennies à venir.

16 Cette question est largement débattue dans l´ opinion du groupe dit de l´article 29 dans la Working document on Data Protection Issues to RFID Technology, en date du 19 janvier 2005, disponible sur: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105.en.pdf qui reprend le considérant 26 de la directive pour conclure que dans la plupart des cas les données créées par les émissions d´ un RFID sont des données à caractère personnel. A notre avis, un tel raisonnement est contestable dans la mesure où la recherche de l´ identité de la personne n´est pas nécessaire pour pouvoir agir vis-à-vis d´elle et qu´on peut dès lors difficilement parler à propos de données relatives à un objet de données à caractère personnel. Par ailleurs, l´exercice de certains droits qui découlent de l´application de la directive s´avère difficile. A noter que des associations comme CASPIAN aux Etats Unis proposent une réglementation des RFID en tant que tels (à cet égard voir le site www.spychips.com/press-releases/right-to-know-bill.html

17 A propos de la parfaite transparence et maîtrise du fonctionnement des anciens terminaux comme le téléphone ou le fax, lire Y. Poullet, J-M. Dinant, *«L´autodétermination informationnelle à l´ère de l´Internet»*, Rapport pour le Conseil de l´Europe , Nov. 2004, en voie de publication, p. 10 et s.

18 Sur le fonctionnement de ces logiciels intrusifs, lire www.clubic.com/actualite-21463-phishing-et-spyware-les-menaces-pesantes-de-2005.html

19 Les organes de normalisation et de standardisation en matière de technologie de l´information et de la communication sont de plus en plus des organes privés échappant au contrôle des organisations publiques.

20 Ainsi, les normes: JPEG pour les photos; EFR pour la voix; MPEG pour les images en mouvements, .. permettent la normalisation de tout signal audible ou visible.

21 En l´état actuel de l´art, la fibre optique, insensible au parasites électromagnétiques, permet des débits de l´ordre de 10Gbits/seconde. Les câbles actuels contiennent plusieurs fibres (de quelques dizaines à quelques centaines). Grâce à la technologie DSL, il est aujourd´hui classique d´atteindre des débits allant jusqu´à quatre mégabits/seconde sans devoir modifier le fil téléphonique classique à paire torsadée et avec un appareillage de quelques dizaines d´Euros. Ceci signifie qu´à terme, il est techniquement possible que la télévision emprunte la voie de l´Internet plutôt que celle du satellite ou de la télédistribution par câble coaxial dédicacé. Des expériences en ce sens sont d´ailleurs en cours dans de nombreux pays. Ceci présente un nouvel enjeu. Actuellement, le satellite et le câble de télédistribution, techniquement, ne permettent pas ou peu à l´émetteur de programme de savoir quels sont les programmes regardés par le consommateur (techniquement, tous les signaux arrivent sur l´ équipement terminal de l´abonné et c´est celui-ci qui choisit celui qu´il veut regarder). Avec la télévision sur Internet, il sera possible de savoir sur une base individuelle qui regarde quoi et même d´injecter de manière ciblée des publicités à des moments précis, toujours sur une base individuelle.

22 A propos de l´IETF, le W3C et l´ICANN comme organes de normalisation privés échappant aux réglementations étatiques, lire P. Amblard, «*Régulation de l´ internet*», Thèse, Bruylant, 2004, p. 70 et s.. J. Reidenberg note avec raison que les standards élaborés par ces organisations deviennent une source normative de la conduite des internautes (J. R. Reidenberg, «*Lex informatica: the formulation of Information Policy rules through Technology*», 76 Texas Law Review, 3 (1998), p. 556 et s.). On notera que le protocole IPV6 qui permettra demain d´identifier de manière stable chaque terminal connecté au réseau est discuté au sein de la seule organisation IETF sans que les Etats ne soient conviés à ce débat. Sur ce protocole, lire: www.telecom.gouv.fr/documents/ipv6/body.htm et les réactions du Groupe de travail de l´article 29 in Avis 2/2002 relatif à l´utilisation d´identifiants uniques dans les terminaux de télécommunication: exemple de l´IPv6, 30 mai 2002, disponible sur le site de la Commission http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2002_fr.htm

23

Working Document on Data Protection issues related to RFID technology, 19 janvier 2005 déjà cité.

[24] Cette notion de profilage pourrait conduire à considérer que la recherche de l´ identité s´ opère alors par référence non à des données administratives (nom, prénom, adresse, etc.) mais par rapport *"à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale»*, comme le permettrait le dernier membre de phrase de l´article 2 a) de la directive . Ainsi, un cookie serait donnée à caractère personnel lorsque le nombre de données collectées grâce au cookie permettrait de constituer une image suffisamment précise de la personnalité de l´ individu peu importe l´aspect considéré (profil économique, psychologique ou physiologique). Cette piste apparaît plus féconde mais elle se heurte au fait que dans l´esprit de la directive ces profils ne sont pas pris pour eux-mêmes et ne constituent des données à caractère personnel que dans la mesure où ils permettent de découvrir l´ identité de la personne concernée.

[25] Le fameux «Right to left alone» défendu par S. Warren et L. Brandeis dans leur article fameux: *«The right to privacy»*, 4 Harvard Law Rev., 193 (1890).

[26] A ce propos, la Recommandation 428 (1970) du Comité d´experts du Conseil de l´Europe portant déclaration sur les moyens de communication de masse et les droits de l´homme, Annales de la Conv. Vol. 13, 1970, p. 65.

[27] Sur cette évolutivité certaine du concept et son caractère essentiel, lire entre autres , L. Burgorgue-Larsen, « *L´appréhension constitutionnelle de la vie privée n Europe», in* Le droit à la vie privée au sens de la Convention européenne des droits de l´ Homme, F.Sudré (éd.), Collection Droit et Justice, n° 63, Bruylant, Nemesis, 2005, p. 72.

[28] Trib. constitutionnel 24 mai 2001, n° 118/1001. Mêmes réflexions de la Cour européenne des droits de l´Homme dans les affaires Guerra et surtout Moreno Gomez (Arrêt du 16 nov. 2004) cette fois à propos d´industries polluantes. Sur ces affaires, J.P. Marguénaud, «*De l´identité à l´épanouissement*», in Le droit au respect de la vie privée au sens de la Convention européenne des droits de l´ Homme déjà cité, p. 220 et s.

[29] Sur cette évolution, notamment, O de Schutter, La vie privée entre droit de la personnalité et liberté, Rev. Trim. Dr. H.(1999), p. 827 et s.

[30] Arrêt Niemetz c. Allemagne, CEDH. 16 décembre 1992, § 29: il s´agissait ici des relations de travail.

[31] Voir à cet égard, S.Gutwirth, «*Privacyvrijheid! De vrijheid om zichzelf te zijn*», Rathenau Instituut, Den Haag, Juin 1998, p. 51 et s.

[32] C´est par ces mots que de Schutter (*art.cité,* p. 839) résume la position de RIGAUX («*La vie privée.Une liberté parmi les autres!»,* Travaux de la faculté de droit de Namur, Bruxelles, Larcier, 1992, p. 120 et s.) et Gutwirth, op .cit.

[33] Comme le note D. Solove (« *The Digital person, Technology and privacy in an Information Age»* , New York University Press, 2004, p. 57 et s.). L´article de WARREN et BRANDEIS part de la constatation des risques d´intrusion dans l´intimité des personnes causés par les premiers appareils photographiques portables.

[34] Il est clair que l´article 8 s´explique d´abord par la volonté d´ éviter toute reproduction de certains agissements de l´ Allemagne nazie.

[35] La loi du Lande de Hesse est sans doute un bel exemple de cette approche, de même que la loi française de 1978, prise en réaction au projet SAFARI.

[36] Th. Leonard, Conflits entre droits subjectifs, libertés civiles et intérêts légitimes, Thèse, Namur, Larcier, 2005, p. 105.

[37] …que le même auteur définit comme: «*le pouvoir d´agir ou de ne pas agir attribué par le droit objectif à chacun en vue de la satisfaction des intérêts qui en forment le but et pour lequel il reçoit du droit objectif les moyens juridiques de défense vis à vis des tiers»* (*op.cit .*, p. 288)

[38] Sur cette notion de droits subjectifs de protection (auxquels le personne protégée ne peut renoncer) distingués des droits subjectifs de disposition (qui constituent des droits de libre disposition pour ceux auxquels ils sont attribués), lire X. dijon, «*Le sujet du droit en son corps- Une mise à l´épreuve du droit subjectif.»,* Thèse, Larcier, 1982.

[39] Ces articles de la charte sont intégralement repris dans le projet de Constitution européenne aux articles II,67 et II 68.

[40]

A cet égard, lire S. Louveaux, M.V. perez-asinari, «*New European Directive 2002/58 on the processing of personal data and the Protection of Privacy in the Electronic Communications Sector* », (2003) CTLR, 5, p. 133; W. maxwell (ed.), *«Electronic Communications: The new EU Framework* : *Booklet I.5: The Communications Data Protection Directive»,* Oceana, Dobbs Ferry, New York, 2002.

[41] Directive 97/66/CE relative aux traitements de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, J.0. 24 Janvier 1998, p. 1.

[42] A ce propos, l´article 1.2. de la Directive note à juste titre: «Les dispositions de la présente Directive précisent et complètent la directive 95/46/CE ….»

[43] C´est tout le débat sur le fameux article 15 de la directive à propos du droit des Etats de demander la conservation des données de trafic. Le débat sur ce thème n´ a pas encore abouti.

[44] La mention de données à caractère personnel n´est pas utilisée. On note ici aussi que la question est abordée sans qu´on s´interroge sur l´existence on non d´un traitement de données à caractère personnel. C´est l´équipement terminal qui en tant que tel est visé et qui fait l´objet de la protection réglementaire. On sait que la question de savoir si les cookies sont des données à caractère personnel est loin d´être tranchée. Cette disposition rend ce débat inutile.

[45] Cet article se fonde sur la disposition de la directive 1999/5/CE (du Parlement européen et du Conseil du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, JOCE n° L 091 du 07/04/1999 pp. 0010 – 0028) qui parmi les «essential requirements» qui doivent être respectés par les producteurs ou distributeurs d´équipements terminaux prévoient outre les questions de sécurité des utilisateurs ou des prestataires du réseau, la protection de la vie privée des utilisateurs.

[46] Directive 2002/21/CE, article 1(d)

[47] Sur ce point, lire J. Grijpink et C. prins, «*Digital Anonymity on the Internet, New Rules for anonymous electronic Transactions?*», 17 *CL&SR* (2001), p. 378 et ss.

[48] A ce propos, lire notamment S. rodota, «Beyond the E.U. Directive: Directions for the Future», in *Privacy: New Risks and opportunities*, Y. poullet- C. de terwangne et P. turner (ed.), Cahier du CRID, n° 13, p. 211 et ss.

[49] Lignes directrices pour la protection des personnes à l´égard de la collecte et du traitement de données à caractère personnel sur les «inforoutes», texte disponible sur le site du Conseil de l´ Europe. Dans le même sens, la recommandation 3/97 du groupe dit de l´article 29 intitulée: «l´anonymat sur Internet». Cf. également l´ avis de la Commission belge de la vie privée pris d´initiative sur le commerce électronique (Avis n° 34/2000 du 22 novembre 2000, avis disponible sur le site de la Commission belge de la vie privée: www.privacy.fgov.be) rappelle à bon escient qu´il existe des mécanismes qui permettent d´authentifier l´émetteur d´un message sans nécessairement l´obliger à s´identifier.

[50] Cf. l´article 8.1 de la directive qui précise que cette présentation doit pouvoir être évitée par un moyen simple et gratuit. Un tel prescrit a des conséquences sur la configuration de l´appareil terminal.

[51] Cf. à cet égard, la recommandation de la CNIL suivant laquelle tout accès à un site marchand doit être possible sans que l´internaute n´ait à s´identifier préalablement (M. georges, Relevons les défis de la protection des données à caractère personnel: l´ Internet et la CNIL, in *Commerce électronique- Marketing et vie privée*, Ph. lemoine (ed.), Paris, LaSer, 1999, p.71 et 72. Cf. également;, le document de travail du groupe dit de l´article 29 à propos des systèmes d´authentification en ligne et en particulier de Netpassport.

[52] En ce sens, la Résolution de la 25ème conférence internationale de Commissaires à la protection des données, prise à Sydney en 2003 (www.privacy.conference2003.org): «chacun…devrait avoir la possibilité de supprimer, désactiver ou détruire les étiquettes»

[53] La qualité des services offerts et des exigences de confidentialité pourrait être l´objet d´un cahier des charges, comme il en est proposé en matière de signatures électroniques. L´agréation d´un «anonymiser» reconnaîtrait son respect du cahier des charges. On peut concevoir que l´agréation ne soit pas requise mais volontaire, équivalent dans ce cas à un label de qualité. .

[54] Cette idée a été reprise par deux lois belges récentes qui obligent un comité sectoriel à établir pour le réseau en lien avec le Registre National (Loi du 8 août 1983 organisant un registre national des personnes physiques modifié par la loi du 25 mars 2003, M.B. 28 mars 2003, art.12 § 1) et celui en lien avec la Banque Carrefour des entreprises (Loi 16 janvier 2003 portant création d´ une Banque Carrefour des entreprises, M.B. 5 fév. 2003, article 19 § 4).

[55] Pour les décideurs privés, le principe est le même sous réserve des intérêts légitimes du maître du fichier (en particulier, le secret des affaires qui pourrait atténuer le devoir d´expliciter la logique suivie).

[56] Recommandation sur les traitements invisibles et automatiques de données à caractère personnel sur Internet réalisés par des logiciels et matériels

[57] Ainsi, dans le document relative aux RFID: Working Document on Data Protection issues related to RFID technology, 19 janvier 2005 déjà cité.

[58] Sans doute, serait-il utile de développer la comparaison entre les modes de régulation de ces deux problématiques: la privacy, d´une part et l´environnement, d´autre part vu les similarités des contextes: caractère transnational des enjeux, dimension technologique importante et la similarité des approches: auto ou co-régulation du secteur, droit à l´information des personnes concernées, principe de sécurité, …

[59] Selon l´expression de J.-M. dinant, «*Law and Technology Convergence in the Data Protection Field* **?** *Electronic threats on personal data and electronic data protection on the Internet*», in E-commerce law and practice in Europe, Ed Ian WALDEN & Julia HORNLE, under the auspices of the Eclip Network, Wood Head Publishing Limited, Cambridge, Avril 2001

[60] Voir à ce sujet, J-M DINANT and E. KEULEERS, *Part 1: «Data protection: multi-application smart cards. The use of global unique identifiers for cross-profiling purposes***»***. Part 2: «Towards a privacy enhancing smart card engineering»*, in *CL & SR*, Vol. 20, n°1, 2004, pp. 22-28, Elsevier, Oxford, 2004.

[61] On souligne que cette volonté de développer les PETS (Privacy Enhancing Technologies) est un des axes majeurs de la politique du Groupe dit de l´article 29 et de la Commission. Un séminaire s´est tenu à cet égard le 4 juillet 2003. On note dans le Rapport de la Commission sur la mise en œuvre de la Directive 95/46/CE établi par la Commission et publié le 15 mai 2003 (COM(2003) 205 final, rapport disponible sur le site de la Commission) que le point 8 des initiatives européennes pour une meilleure application de cette directive est précisément la promotion des technologies renforçant la protection de la vie privée: «*La Commission, note le rapport, travaille déjà, dans le domaine des technologies renforçant la protection de la vie privée, notamment au niveau de la recherche comme par exemple, les projets RAPID et PISA… Elle invite les autorités nationales de contrôle à poursuivre les discussions sur la question des technologies permettant de renforcer la protection de la vie privée et de réfléchir sur les mesures que les autorités nationales de contrôle pourraient prendre ...*»:

[62] Sur ce point, nos réflexions in «*Comment «réguler» la protection des données? Réflexions sur l´ internormativité?* » , Mélanges P. delnoy, Larcier, 2005, à paraître. A cet égard, relevons que les technologies qualifiées de Pet peuvent s´avérer «privaticides», lire sur ce point le débat à propos du P3P, entre rotenberg et lessig in «*Fair Information Practices and the Architecture of Privacy (Whart larry Doesn´t Get)*», 2001 Stanford Technology Law Review, 1.

[63] On songe bien évidemment à des systèmes de labellisation ou à des agréments donnés par l´autorité publique à certaines entreprises.

[64] A ce sujet, J-M dinant , «*Le visiteur visité***,** *Quand les éditeurs de logiciel Internet passent subrepticement à travers les mailles du filet juridique»,* in *Lex Electronica*, vol. 6, n°2, hiver 2001

[65] Article 2 – Accès illégal: Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l´accès intentionnel et sans droit à tout ou partie d´un système informatique. Une Partie peut exiger que l´infraction soit commise en violation des mesures de sécurité, dans l´intention d´obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

[66] Article 3 – Interception illégale: Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l´interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l´intérieur d´un système informatique, y compris les émissions électromagnétiques provenant d´un système informatique transportant de telles données informatiques. Une Partie peut exiger que l´infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

[67] Voir à ce sujet l´excellent article de Thierry leonard, « *E- commerce et protection des données à caractère personnel: Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet*» disponible sur www.droit.fundp.ac.be/Textes/Leonard1.pdf

[68]

En d´autres termes, nous soutenons que le placement d´un numéro identifiant dans un terminal de télécommunication ou le simple accès à ce numéro ou à un autre identifiant du terminal constituent un accès majoritairement non autorisé. Il n´importe pas, dans ce cadre légal, de jauger la proportionnalité de tels procédés. L´autorisation demeure un acte positif qui se distingue de l´acceptation qui peut se déduire d´un silence éventuel ou de l´absence d´opposition.

[69] Ces conclusions s´inspirent grandement des conclusions du rapport que l´ auteur et J. -M dinant ont écrit pour le Conseil de l´ Europe: «*L´autodétermination informationnelle à l´ ère de l´ Internet*», Eléments de réflexion sur la Convention n° 108 destiné au travail futur du Comité consultatif (T-PD), Rapport en voie de publication, novembre 2004.

[70] C. clarke, «The answer to the machine is in the machine», in *The future of Copyright in a digital Environment,* B. Hugenholtz (ed.), Kluwer, 1996, p. 139 et ss.

[71] Recommandation n° R (99)5, point III; 1, 2 et 4

[72] Cf à ce propos, l´avis de la Commission belge n° 34/2000 à propos de la protection des données dans le cadre du commerce électronique.

[73] A ce propos les démarches opérées par le Groupe dit de l´article 29 et relatées in Note d´information générale concernant le rapport du CEN/ISSS sur la normalisation au service de la protection de la vie privée en Europe (CEN, Centre européen de normalisation) (Avis 1/2002),30 mai 2002, note disponible sur le site de la Commission déjà cité et surtout la résolution prise à Wroclaw lors de la 26ème conférence internationale de protection de la vie privée et des données à caractère personnel qui consacre les efforts de l´ ISO en la matière: «Whereas the International Working Group on Data Protection in Telecommunications at their 35th meeting in Buenos Aires on 14-15 April 2004 has adopted a Working Paper on a future ISO Privacy Standard;» «Whereas the International Conference of Data Protection and Privacy Commissioners (hereafter «Conference») wishes to support the development of an effective and universally accepted international privacy technology standard and make available to ISO its expertise for the development of such a standard;…» Sur le thème standardisation et vie privée, on lira P. Rosensweig et A .Kochems,«Data Protection: Safeguarding Privacy in a New Age of Technology», 23 mars 2005 publié in www.heritage.org/Research/HomelandDefense/lm16.cfm

Rechtsgebiet: Datenschutz
Erschienen in: Jusletter 3. Oktober 2005
Zitiervorschlag: Yves Poullet, Pour une troisième génération de réglementations de protection des données, in: Jusletter 3. Oktober 2005
Internetadresse: http://www.weblaw.ch/jusletter/Artikel.asp?ArticleNr=4213